REMARKS

This application has been reviewed in light of the Office Action dated February 27, 2009. Claims 1 and 3–14 are pending in the application. Claims 4 and 8–12 have been amended to resolve informalities. No new matter has been added. Reconsideration of the rejection in light of the arguments and the amendments is respectfully requested.

Objections to the Claims

The Examiner objects to claim 4, noting that claim 4 was amended in the previous response, and that the claim heading did not indicate that fact. The Examiner further objects to claim 4, noting an inconsistency in the "key" nomenclature. Claim 4 has been amended to render its language consistent with claim 1, and has furthermore been properly designated as "currently amended" in accordance with 37 C.F.R. 1.121(c). It is believed that this resolves the Examiner's objection.

The Examiner further objects to claims 8–12, stating that the term "mechanism" is unclear with regard to whether the claims should be interpreted as methods or as systems. Applicants have amended claims 8–12 to specifically recite key synchronization systems. It is believed that this revolves the Examiner's objections.

Claim Rejections under 35 U.S.C. 103(a)

Claims 1, 7–8, and 13 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,526,506 to Lewis (hereinafter "Lewis") in view of U.S. Patent Publication No. 2004/0081320 to Jordan et al. (hereinafter "Jordan").

Claim 1 recites, *inter alia*, "generating a new encryption key at the access point." The Examiner asserts that Lewis discloses this element in its discussion of how an access point may be instructed to use a new or different key.

However, key management is handled entirely by Lewis's key distribution server 76, e.g., Lewis, col. 8, line 35- col. 9, line 65 . Specifically, an encryption key generator is used for periodically generating a new encryption key, which is provided to the access points (see Lewis, col. 9, lines 41-46). Thus, Lewis's access points 54 merely accept the keys from the key distribution server 76. Indeed, even the portion of Lewis cited by the Examiner (i.e., col. 12, lines 43-44) refers only to instructing the access points to change keys — nothing is said about generating the key in an access point. It is therefore clear that Lewis does not teach generating encryption keys at the access points.

It should also be noted that, although the Examiner does not rely on Jordan for this purpose, Jordan fails to cure the deficiencies of Lewis. Jordan makes no mention of access points, and as a result, cannot disclose or suggest generating encryption keys at access points. Therefore, Lewis and/or Jordan, taken alone or in combination, fail to disclose or suggest generating encryption keys at an access point.

Claim 1 further recites, "indicating a decryption failure for a data frame received from the station when the encryption key used by the station does not match the current encryption key, wherein a data frame that failed to decrypt using the current encryption key is decrypted using the old encryption key." The Examiner asserts that Lewis discloses this element in FIG. 7, showing the procedure taken by the access points when a message cannot be decrypted with the current key.

However, Lewis at no point discloses or suggests indicating such a decryption failure. Indeed, an inspection of FIG. 7 shows that Lewis's access points simply pass or block messages that do not match the encryption key. There is no discussion of providing any indication that a failure occurred. Furthermore, the simple fact that packets get blocked cannot be construed as providing an indication.

Again, it is worth noting that Jordan fails to cure the deficiencies of Lewis in this respect. Jordan does not provide any indication of a decryption failure when a data frame fails to decrypt using the current key. Therefore, Lewis and/or Jordan, taken alone or in combination, fail to disclose or suggest "indicating a decryption failure for a data frame received from the station when the encryption key used by the station does not match the current encryption key, wherein a data frame that failed to decrypt using the current encryption key is decrypted using the old encrypted key."

Claim 8 recites, *inter alia*, "maintaining an old encryption key and a new encryption key through a key rotation interval ..." The Examiner asserts that Lewis discloses the old encryption key by using the old encryption key to send a new encryption key, and that Lewis discloses the key rotation interval by periodically changing keys.

However, it must be noted that the claim recites maintaining an old encryption key and a new encryption key through a key rotation interval. This feature of maintaining both keys through a certain interval is neither disclosed nor suggested in the cited art. Instead, Lewis discloses using the old key once, and only once, when it broadcasts the message containing the new key. Lewis makes no further use of the old key after the new key has been sent. As a result, it cannot be said that Lewis in any way discloses or suggests maintaining both the old key and the new key through any interval. As soon as Lewis's new key is sent, the old key becomes obsolete.

Indeed, Lewis cannot be described as maintaining an old key and a new key simultaneously. The Examiner points to one use of the old key, namely, for communicating the new key (Lewis, col. 12, lines 44-47). However, this specific use of the old key takes place before the new key goes into effect. After the new key has been received and stored, "the mobile terminal 66 uses the new ENCRYPT key by providing the new ENCRYPT key to the encryption engine 94" (Lewis, col. 12, lines 53-58). The cited sections of Lewis do not teach or suggest maintaining both the old and new keys during any interval.

Jordan fails to cure the deficiencies of Lewis. For example, FIG. 8 of Jordan depicts a technique strikingly similar to Lewis, in which an old password is used to encrypt a message containing the new password, and wherein subsequent communications are encrypted using the new password. Furthermore, Jordan's FIGS. 10-11 (cited by the Examiner) also do not teach maintaining both old and new keys during an interval. Instead, they only teach reverting back to an old password key during a resynchronization process. Thus, Applicants submit that Lewis and/or Jordan, taken alone or in combination, fail to disclose or suggest maintaining an old encryption key and a new encryption key through a key rotation interval.

For at least the above reasons, it is believed that claims 1 and 8 are in condition for allowance. Since claims 7 and 13 depend from claims 1 and 8 respectively and include all of the elements of their parent claims, it is also believed that claims 7 and 13 are in condition for allowance. Reconsideration of the rejection is earnestly solicited.

Claims 3, 4, 9, and 14 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Lewis, in view of Jordan and further in view of U.S. Patent No. 7,293,289 to Loc et al. (hereinafter "Loc").

Claims 3, 4, 9, and 14 depend from claims 1 and 8 and include all of the elements of their parent claims. Since there is no showing that Loc cures the above-discussed deficiencies of Lewis and Jordan, Applicants submit that Lewis, Jordan, and/or Loc, taken alone or in any combination, fail to disclose or suggest all of the elements of claims 3, 4, 9, and 14. Reconsideration of the rejection is earnestly solicited.

Claims 5–6 and 10–12 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Lewis, in view of Jordan and further in view of U.S. Patent No. 6,118,869 to Kelem et al. (hereinafter "Kelem").

Claims 5–6 and 10–12 depend from claims 1 and 8 and include all of the elements of their parent claims. Since there is no showing that Kelem cures the above-discussed deficiencies of Lewis and Jordan, Applicants submit that Lewis, Jordan, and/or Kelem, taken alone or in any combination, fail to disclose or suggest all of the elements of claims 5–6 and 10–12. Reconsideration of the rejection is earnestly solicited.

In view of the foregoing amendments and remarks, Applicants submit that all the claims now pending in the application are in condition for allowance. Early and favorable reconsideration of the case is respectfully requested.

Respectfully submitted,
Zhang et al.

May 27, 2009
Date

/Wan Yee Cheung/
Wan Yee Cheung
Attorney for Applicants
Reg. No. 42,410

Patent Operations
Thomson Licensing LLC
P.O. Box 5312
Princeton, NJ 08540-5312